881

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 June 2005 (02.06.2005)

PCT

(10) International Publication Number
WO 2005/050414 A1

(51) International Patent Classification[7]: G06F 1/00, H04L 29/06, 12/26

(21) International Application Number: PCT/EP2003/012090

(22) International Filing Date: 30 October 2003 (30.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: TELECOM ITALIA S.P.A. [IT/IT]; Piazza degli Affari, 2, I-20123 Milano (IT).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BRUSOTTI, Stefano [IT/IT]; Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT). CODA ZABETTA, Francesco [IT/IT]; Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT).

(74) Agents: GIANNESI, Pier, Giovanni et al.; Pirelli & C. S.p.A., Viale Sarca, 222, I-20126 Milano (IT).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

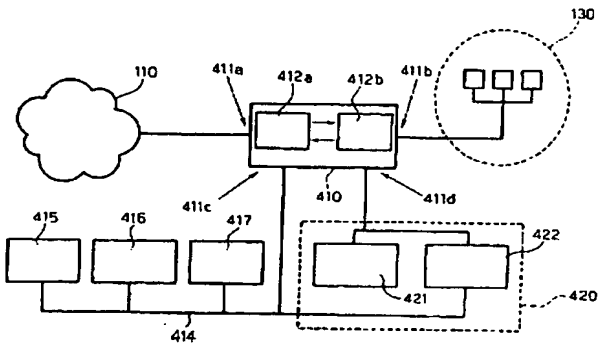
(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ,*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR INTRUSION PREVENTION AND DEFLECTION,



(57) Abstract: A system for preventing intrusion in communication traffic with a set (130) of machines in a network includes a data base (415) having stored therein patterns representative of forbidden communication entities as well a firewall module (412a) configured for blocking forbidden communication entities in the traffic as identified by respective patterns included in the data base (415). The system further includes another data base (416) having stored therein patterns representative of allowed communication entities for communication with said set of machines (130) and a test system (420) including test facilities (421) replicating the machines in said set (130). A communication module (410) is provided configured for allowing (411b) communication of allowed communication entities as identified by respective patterns included in the other data base (416). Unknown communication entities as identified by respective unknown patterns not included in either of said data base (415) and said further data base (416) are directed (411d) to the test system (420) and run on the test facilities (421) therein to detect possible adverse effects of such unknown communication entities on the test system. The system is further configured so that: i) in the presence of an adverse effect, the unknown communication entity leading to the adverse effect is blocked by the firewall module (412a), and ii) in the absence of an adverse effect, communication of the unknown communication entity failing to lead to said adverse effect is allowed.

WO 2005/050414 A1

TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.